CNS-105-2 Critique #2 : The Tangled Web of Password Reuse

A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. "The Tangled Web of Password Reuse." In NDSS, 2014.

電機三　徐彥旻　b03901027

Summary

本篇利用之前洩漏出來的密碼資料，以及問卷調查，分析使用者如何在不同的網站上使用密碼——四成以上的人會在不同的網站上使用完全相同的密碼。

並且，為了進一步凸顯相關的安全問題，基於使用者的習慣，設計簡單的猜測密碼演算法進行實驗，其結果為：在已知其一密碼的情況下，可以在一百個嘗試內破解百分之三十的同使用者的不同密碼。

最後，提出建議，希望能建立安全的線上服務，讓使用者能確認他們的密碼不會那麼容易被猜到，或者是在各個網站設定密碼的時候，就能利用本篇提出的方法，建議使用者不要在其他網站使用容易被猜到的密碼。

Strength

1. 以分析既有的洩露密碼以及問券調查兩種方式確認了「四成到五成的使用者會在不同的網站上用同樣的密碼」。
2. 設計出猜測密碼的方式，驗證了就算不是用同樣的密碼，也有相當比例的使用者用過於簡單的方式設定新密碼，凸顯此一安全問題。

Weakness

密碼還是很難記憶，這篇論文並沒有解決它所提到的 *password fatique* 的問題

Reflection

1. 從這篇論文當中，學到了使用者如何設計、管理密碼的實際情形，也與自己的使用經驗大致相同。並且瞭解相關的安全問題的嚴重程度。
2. 如果有機會得到資料的話，或許也可以用機器學習或深度學習的技術來做預測，因為很多套件已經很普遍了，比如 Keras, Tensorflow 等等，對於可能的攻擊者來說也算是方便的工具，驗證這樣的新技術會不會造成安全上的問題也是值得探究的。
3. 對於 password fatique，跟據問卷調查的結果，約有一半的人維持三到四組密碼，針對這群人，在不讓他們記更多密碼的前提之下，建議(1)讓這三到四組密碼互相猜不到，以及(2)對於想要有高安全性的網站，不重複使用密碼，例如使用者有四組密碼，那他其中三組密碼可以分別只用在他認為最重要的三個網站上，剩下一

組給不太重要的網站使用，如此一來就算最後一組被人知道了，造成的損害也是比較小的。